October 2022

Document title: **[ACCEPTABLE USE POLICY– October 2022]**

Approval date: **[August 2018]**

Purpose of document:
[The purpose of this policy is to outline the acceptable use of AUC IT resources at AUC. These rules are in place to protect the staff, faculty, students, and AUC community. Inappropriate use exposes AUC to risks, including information disclosure, virus attacks, compromise of network systems and services, and legal issues.]

Office/department responsible: **[Office of Information Security]**
Approved by: **[Ms. Nagwa Nicola, Chief Technology Officer]**

Document classification level: **[PUBLIC]**

Document accessible: **[** https://www.aucegypt.edu/about/university-policies**]**

Document includes: **[Policy]**

Related documents/see also: **[AUC Policies,**
https://www.aucegypt.edu/about/universitypolicies**]**

Acceptable Use Policy

Policy Statement

This policy is a means of explaining the acceptable and non-acceptable behavior that the AUC community and users should adhere to when using AUC IT resources. Complying with this policy will help the AUC community to be more secure from an IT perspective as well as decreasing the risks associated with the usage of AUC IT resources.

Reason for Policy/Purpose

The purpose of this policy is to outline the acceptable use of AUC IT resources at AUC. These rules are in place to protect the staff, faculty, students, and AUC community. Inappropriate use exposes AUC to risks, including information disclosure, virus attacks, compromise of network systems and services, and legal issues.

Who Approved This Policy

Chief Technology Officer Ms. Nagwa Nicola

Who Needs to Know This Policy

This policy applies to visitors, staff, faculty, students, alumni, contractors, consultants, temporaries, other workers, and any person who uses AUC IT resources at AUC, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by AUC and to any equipment that uses AUC IT resources.

Web Address for this Policy

https://www.aucegypt.edu/about/university-policies

Contacts

Responsible University Official: Wessam Maher, Chief Information Security and Risk Officer.
Responsible University Office: Office of Information Security.
If you have any questions on the policy, you may send an email to infosec@aucegypt.edu

Definitions

Term (alphabetical order)	Definition as it relates to this policy
AUC IT Resources	Any IT services, IT equipment or any IT means of communication provided by AUC
AUC Community	This term refers to the AUC faculty, staff, Alumni and students or any person or entity that deals with AUC technology services

Policy/Procedures

1. AUC Staff and faculty should be aware that the data they create on the University systems remains the property of AUC.

2. AUC will exercise and perform all feasible activities to govern information confidentiality but cannot guarantee the confidentiality of the information stored on any electronic device belonging to AUC.
3. The Information Security Office recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within AUC may monitor equipment, systems, and network traffic at any time with permission from the Information Security Office.
5. AUC reserves the right to audit IT resources on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information:

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
2. All IT equipment should be secured with a password-protected auto-lock with the automatic activation feature set at 5 minutes or less or by logging off when the host will be unattended.
3. As the information contained on portable computers, memory sticks, or any portable device storing sensitive information is especially vulnerable, special care should be exercised to keep this information secured.
4. All IT equipment used by AUC contractors, guests, faculty, staff, and students that are connected to the AUC Network locally or remotely, whether owned by themselves or AUC, should have their computer software continually updated. Approved anti-malware-scanning software with an updated database, Host Intrusion Prevention System and firewall software of this equipment must be constantly updated.
5. Users must use extreme caution when browsing and opening email attachments or clicking on web links received from any sender as they may contain viruses, Trojans, or malicious programs.

Unacceptable Use:

The following activities are, in general, prohibited. AUC Personnel may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a user authorized to engage in any activity that is illegal under local or international law while utilizing AUC-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, confidentiality, or similar laws or regulations, including, but not limited to the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by AUC.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which AUC or the end-user does not have an active license are strictly prohibited.
3. Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, email bombs, hacking tools, etc.).
4. Revealing your account password to others or allowing the use of your account credentials by others under any circumstances. This includes family and other household members when work is being done at home or in dorms/housing.
5. Affecting trails for security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data where the user is not the intended recipient or logging into a server or account that the user is not expressly authorized to access - unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, spoofing, denial of service, and forged routing information for malicious purposes.
6. Port scanning or security scanning is expressly prohibited unless prior authorization is secured from the Information Security Office.
7. Executing any form of IT traffic monitoring which will intercept data not intended for the user's host unless this activity is a part of the user's normal job/duty.
8. Circumventing user authentication or security of any host, network, or account.
9. Interfering with or denying service to any host (for example, denial of service attack).
10. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
11. Providing any information about or lists of the AUC community to parties outside AUC without prior approval from the Chief Technology Officer.
12. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
13. Any form of harassment via email, telephone, paging, or other electronic means, whether through language, frequency, or size of messages.
14. Unauthorized use, or forging, of email header information.
15. Solicitation of email for any other email address other than that of the poster's account, with the intent to harass or to collect replies.
16. Posting the same or similar non-business-related messages to large numbers of recipients.
17. Using AUC IT resources in a non-AUC business domain.
18. Any use of Peer-to-Peer programs. (e.g.:edonkey, bittorrent, etc.). Kindly refer to the AUC Policy Banning Peer-To-Peer file sharing in accordance with The Higher Education Opportunity Act of 2008.
19. Installation of any IT services/equipment without written assessment and approval from the Information Security Office.
20. Spoofing/phishing of websites, emails, AUC services.
21. Entering false or fake information on IT systems or resources.
22. Unauthorized access to IT systems data centers and facilities.
23. Performing any sort of reconnaissance, hacking, or penetration testing activities on any AUC IT resource.
24. Bypassing or trials to bypass any blocked internal or external IT service or website.

25. Abusive usage behavior for any IT service.

Enforcement:

Any user found to have violated this policy (or part thereof) may be subject to disciplinary action, up to and including termination of employment or dismissal from the University

Forms/Instructions

None

Related Information

https://www.aucegypt.edu/about/university-policies

Appendices *(optional)*

None

History/Revision Dates

Origination Date:	September 2012
Last Amended Date:	June 15th, 2018
Last Review Date:	October, 2022
Next Review Date:	October, 2025